IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-20. (Canceled)

21. (Previously Presented) A system for detecting intrusions on a host, comprising:

a sensor for collecting information from a logfile located on the host; and

an analysis engine embodied in a computer security system and coupled to the sensor for analyzing the logfile and including a time decay function;

wherein the analysis engine is configured to use the time decay function to compute a suspicion value for an entry in the logfile including by using the time decay function to compute a probability for an end of a session with which the entry is associated.

22. (Original) The intrusion detection system as recited in claim 21, wherein the logfile is sulog and the session is an su session.

23-24. (Canceled)

25. (Previously Presented) A method for detecting intrusions on a host, comprising:

collecting information from a logfile located on the host; and

analyzing the logfile, including by using a time decay function to compute a suspicion value for an entry in the logfile including by computing a probability for an end of a session with which the entry is associated.

26. (Previously Presented) A method as recited in claim 25, wherein the logfile is sulog and the session is an su session.

27. (Previously Presented) A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

collecting information from a logfile located on the host; and

analyzing the logfile, including by using a time decay function to compute a suspicion value for an entry in the logfile including by using the time decay function to compute a probability for an end of a session with which the entry is associated.

28. (Previously Presented) A computer program product as recited in claim 27, wherein the logfile is sulog and the session is an su session.